Samba

Table des matières

Liste de tableaux

1. PROCESSUS

nmbd. entre en jeu lors de l'exploration du réseau (résolution de nom, ...). Utilise le protocole UDP.

smbd. prend en charge toutes les connexions TCP/IP (services de fichiers, imprimantes, ...) et l'authentification.

winbindd. utilisé lorsque samba apparient à un domaine NT ou ADS. Prend en charge l'authentification et les relations d'approbation.

2. CONFIGURATION

Samba utilise le fichier `smb.conf` et des fichiers binaires situés dans `/usr/local/samba/var/locks/` (fichiers `tdb`). Ce dossier est contrôlable à l'aide du paramètre `lock directory` dans `smb.conf`.

Niveaux de configuration :

- partages ;
- exploration ;
- authentification ;
- impression.

Les *noms des paramètres* sont **insensibles** à la casse. La règle est moins claire pour la *valeur de ces paramètres* puisque par exemple les chemins sont sensibles à la casse sous Unix.

2.1. Modification de la configuration

- À chaque nouvelle demande de connexion, un fork du processus `smbd` est créé. Le processus fils relit les fichiers de configuration et prend donc en compte toute modification.
- Une fois démarré, le processus `smbd` principal vérifie toutes les trois minutes si les fichiers de configuration ont été modifiés.
- Un administrateur peut forcer la relecture des fichiers de configuration (`reload-config message` via `smbcontrol`).
- Le paramètre `printcap cache time` règle l'exploration de nouvelles imprimantes.

2.2. Conclusion

1. Travailler sur une copie du fichier `smb.conf` ;
2. Vérifier sa syntaxe ;
3. Remplacer `smb.conf`.

Remarque. Le fichier `smb.conf` étant lu régulièrement, il est préférable qu'il soit le plus petit possible. Il faut donc travailler sur, par exemple, `smb.conf.master` (fichier dans lequel on place toutes les instructions avec leur commentaire) et générer le fichier `smb.conf` à l'aide de la commande : `testparm -s smb.conf.master > smb.conf`

3. smb.conf

3.1. Variables

Chaque nouvelle demande de connexion étant prise en charge par un processus nouveau, il est possible de déterminer un paramétrage unique pour chaque client grâce à l'utilisation de variables (voir liste page 87).

Exemple 1.

```
[pub]
    path = /home/ftp/pub/%a
```

le partage `pub` pointe vers un dossier sur le serveur dépendant du type d'os du client.

Exemple 2.

```
[homes]
    path = /export/smb/home/%U
```

les dossiers personnels accessibles via Samba pointent vers un dossier dépendant du nom de l'utilisateur du client.

3.2. Fichier de configuration

Paramètre	Valeur	Description	Défaut	Portée
`config file`	string	fichier à utiliser à la place de celui-ci	None	Global
`include`	string	inclure le contenu de ce fichier dans celui-ci	None	Global
`copy`	string	permet de cloner la configuration d'un partage	None	Share

Tableau 1. Fichier de configuration

config file.

Exemple 3.

```
[global]
    config file = /etc/samba/smb.conf.%m
```

indique d'utiliser un fichier de configuration dépendant du nom NETBIOS du client. Si ce fichier n'existe pas, cette ligne est ignorée.

include.

Exemple 4.

```
[global]
    include = /usr/local/samba/lib/smb.conf.%m
```

permet de redéfinir certains paramètres en fonction du nom NETBIOS du client.

copy.

Exemple 5.

```
[basic]
    read only = no
    browseable = yes
    available = no
[data]
    copy = basic
    available = yes
    path = /data
```

3.3. Serveur

Paramètre	Valeur	Description	Défaut	Portée
`netbios name`	string	nom NETBIOS du serveur	host-name	Global
`workgroup`	string	nom NETBIOS du groupe de travail (ou du domaine)	Work-group	Global
`serveur string`	string	chaîne de caractère	samba %v	Global

Tableau 2. Serveur

3.4. Partage

Paramètre	Valeur	Description	Défaut	Portée
`path (directory)`	string	dossier Unix (pour les fichiers ou le spool d'impression)	`/tmp`	Share
`comment`	string	commentaire	None	Share
`volume`	string	nom du volume pour le partage	None	Share
`read only`	boolean	le client est-il autorisé à écrire dans le partage ?	yes	Share
`writable` (ou `write ok` ou `writeable`)	boolean	l'inverse de `read-only` (équivalent à `read-only = no`)	no	Share

Tableau 3. Partage

3.5. Réseau

Paramètre	Valeur	Description	Défaut	Portée
`hosts allow` (`allow hosts`)	string	clients autorisés à se connecter à Samba	None	Share Global
`hosts deny` (`deny hosts`)	string	clients interdits de connexion	None	Share Global
`interfaces`	string	interfaces réseau qu'écoute samba	Toutes les inter-faces	Global
`bind interfaces only`	boolean	indique à Samba de n'écouter que les interfaces spécifiée par `interfaces`	No	Global

Tableau 4. Réseau

Le comportement de `hosts allow` et `hosts deny` est opposé à celui attendu. Leur positionnement dans la section `global` prend le pas sur toute apparition dans la définition d'un partage.

3.6. Serveurs virtuels

Idée. Faire apparaître le serveur Samba comme plusieurs serveurs différents proposant des services différents.

Les clients Win 9x envoient leur demande de connexion au serveur **(port 139)** en se basant sur le protocole NETBIOS (nom qui fait donc parti de la trame que reçoit le serveur). Un administrateur peut utiliser la variable %L pour établir plusieurs fichiers de configuration.

Exemple 6.

```
[global]
    netbios name = PIGEON
    netbios aliases = SEAGULL PELICAN
    server string = Engr Dept Server (Samba %v)
    workgroup = GARDEN
    include = /usr/local/samba/lib/%L.conf
```

Les clients CIFS (win2000, XP, ...) n'utilisent pas, par défaut, la couche NETBIOS et le nom NETBIOS du serveur n'est pas utilisable (il ne fait pas parti de la trame que reçoit le serveur). De plus, le port utilisé, par défaut, par ces clients est le 145 (samba écoute donc aussi ce port).

Il est possible de forcer les clients CIFS à utiliser le port 139 (et donc la couche NETBIOS) en obligeant Samba à n'écouter que le port 139.

Exemple 7.

```
[global]
    netbios name = PIGEON
    netbios aliases = SEAGULL PELICAN
    server string = Engr Dept Server (Samba %v)
    workgroup = GARDEN
    smb ports = 139
    include = /usr/local/samba/lib/%L.conf
```

Pour faire de la virtualisation sur le port 145 (et donc uniquement avec des clients CIFS), il faut utiliser **plusieurs IP** (donc interfaces, qu'elles soient réelles ou virtuelles).

Exemple 8.

```
[global]
    netbios name = PIGEON
    workgroup = GARDEN
    include = /usr/local/samba/lib/%i.conf
```

et au niveau du serveur DNS

```
; Bind 9 address entries
pigeon IN A 192.168.1.10
seagull IN A 192.168.1.11
pelican IN A 192.168.1.12
```

3.7. Fichiers de log

Exemple 9.

```
[global]
    log level = 1
    log file = /var/log/samba/log.%m
    max log size = 50
```

Le niveau peut varier de 0 à 10. Le niveau 0 ne fournit que les messages d'erreurs critiques, le niveau 1 fournit les informations de connexion. En pratique se limiter aux niveaux 1, 2 et 3.

Remarque. On peut personnaliser le fichier par ordinateur, utilisateur, ...

Remarque. Si on utilise `log.%m`, deux fichiers de log seront créés, le premier nommé à partir de l'IP, le second utilisant le nom de la machine. C'est du à l'utilisation du port 445 par les nouveaux clients Windows et donc la non utilisation de la couche NETBIOS (voir la partie sur la virtualisation).

4. COMPTES UTILISATEURS, AUTHENTIFICATIONS ET AUTORISATIONS

4.1. Les différents modes de sécurité

Paramètre	Valeur	Description	Défaut	Portée
`security`	user ads domain share server	modes d'authentification utilisés pour répondre aux différentes requêtes.	user	Global

Tableau 5. Les différents modes de sécurité

Les modes `share` et `server` sont obsolètes et ne doivent plus être utilisés. Ils ne sont conservés qu'à des fins de compatibilité.

4.2. Accès anonyme à un partage en mode `user`

En principe, accéder à un partage nécessite l'enchaînement « *authentification* — *autorisation* ». Le problème ici est : comment autoriser sans authentifier ?

Paramètre	Valeur	Description	Défaut	Portée
`guest account`	username	compte Unix utilisé par smbd lorsque l'accès «invité» est activé au niveau d'un partage	nobody	Global
`guest ok`	boolean	active (ou pas) l'accès «invité» dans le partage	no	Share
`guest only`	boolean	si activé, smbd considère que tout utilisateur accédant au partage est authentifié sous le compte Unix définit par `guest account`	no	Share
`map to guest`	never, bad password, bad user, bad uid	détermine si, malgrè un echec lors de l'authentification (et en fonction du type de l'échec) une autorisation est possible en tant qu'«invité» (il faut `guest ok = yes` au niveau du partage bien sur)	never	Global

Tableau 6. Accès anonyme à un partage

Valeur	Portée
`never`	autorisation refusée si échec de l'authentification
`bad password`	si le compte de l'utilisateur existe mais que le mot de passe donné lors de l'authentification ne correspond pas à celui attendu, l'accès est autorisé en tant qu'«invité» (et non pas donc sous l'identité du l'utilisateur).
`bad uid`	Valide seulement pour les serveurs membres (`security = ads` ou `security = domain`). L'accès est autorisé si l'authentification sur le domaine a réussi mais qu'il n'existe pas de compte local correspondant sur le serveur.
`bad user`	autorise l'accès en tant qu'«invité» si le compte est inconnu de Samba

Tableau 7. Paramètre `map to guest`

Exemple 10.

```
[global]
    netbios name = OAK
    workgroup = GARDEN
    server string = Public access file server
    security = user
    map to guest = bad user
    guest account = smbguest
[public]
    path = /export/public
    guest ok = yes
    read only = no
```

Avant d'utiliser `map to guest`, il faut comprendre qu'en mode `user`, il n'existe qu'*une seule session d'authentification*. Une fois l'utilisateur authentifié en tant qu'invité, il conserve cette identité pour tous les partages qu'il visite sur le serveur (que ceux-ci autorisent ou pas l'accès public).

Si l'on souhaite vraiment héberger des partages publics et d'autres à accès restreint, une des méthodes est la virualisation : une des identités du serveur est destinée aux partages publics, une autre peut être utilisée pour les partages à accès restreint (`map to guest` peut prendre différentes valeurs dans chaque serveur virtuel).

never.

1. un utilisateur n'appartenant pas au domaine ne voit pas le serveur ;

2. un utilisateur du domaine, ayant donné un mauvais mot de passe, ne voit pas le serveur ;
3. un utilisateur du domaine correctement authentifié voit le serveur et peut accéder aux partages.

bad user.

1. un utilisateur n'appartenant pas au domaine voit le serveur, un mot de passe est demandé lors de l'accès à un partage ;
2. un utilisateur du domaine, ayant donné un mauvais mot de passe, ne voit pas le serveur ;
3. un utilisateur du domaine correctement authentifié voit le serveur et peut accéder aux partages.

bad password.

1. un utilisateur n'appartenant pas au domaine voit le serveur, un mot de passe est demandé lors de l'accès à un partage ;
2. un utilisateur du domaine, ayant donné un mauvais mot de passe, un mot de passe est demandé lors de l'accès à un partage ;
3. un utilisateur du domaine correctement authentifié voit le serveur et peut accéder aux partages.

4.3. Mots de passe et authentification

4.4. Identifiant de sécurité

Tout objet (utilisateur, groupe, machine) est identifié de façon unique à l'aide d'une chaîne de caractère (SID), comme :

$$S-1-5-21-3489264249-1556752242-1837584028-1003$$

À partir d'un SID, il est impossible de déterminer de quel type d'objet il s'agit.

Le dernier nombre 1003 constitue (ce n'est pas tout à fait vrai) le RID. Lorsqu'on retire le RID au SID, on obtient l'identifiant de sécurité du domaine, accessible en ligne de commande :

Exemple 11.

```
root# net getlocalsid
SID for domain RAIN is : S-1-5-21-3489264249-1556752242-1837584028
```

4.5. Stockage des comptes

`passdb backend = smbpasswd`.

Les comptes sont conservés dans un fichier texte au format `username:uid:lanman_hash:nt_hash:flags:pw_lct`

Exemple 12.

```
[global]
    security = user
    encrypt passwords = yes
    passdb backend = smbpasswd:/etc/smbpasswd
```

`passdb backend = tdbsam`.

Les comptes sont conservés dans une base de donnée élémentaire. C'est la solution conseillée lorsqu'on construit un PDC sans BDC (puisqu'il n'y a pas de réplication possible).

Exemple 13.

```
[global]
    security = user
    encrypt passwords = yes
    passdb backend = tdbsam:/etc/passdb.tdb
```

`passdb backend = ldapsam`.

Paramètre	Valeur	Description	Défaut	Portée
`ldap admin dn`	DN	le DN de l'entrée de l'annuaire ayant les droits de lecture et de modification	,,,,	Global
`ldap replication sleep`	integer (en milli-secondes)	délai pour la réplication de l'annuaire	1000	Global
`ldap ssl`	off start_tls	couche de transport (ssl ou pas) à utiliser lorsqu'on indique pas ldaps dans l'URI de `ldapsam`	off	Global
`ldap suffix`	DN	suffixe base de toute recherche dans l'annuaire	,,,,	Global
`ldap group suffix`	DN	sufixe base de la recherche dans la branche de l'annuaire des groupes	,,,,	Global
`ldap idmap suffix`	DN	suffixe base de la recherche dans la branche de l'annuaire réservée à `winbindd`	,,,,	Global
`ldap machine suffix`	DN	suffixe base de la recherche dans la branche de l'annuaire des machines	,,,,	Global
`ldap user suffix`	DN	suffixe base de la recherche dans la branche de l'annuaire des utilisateurs	,,,,	Global
`ldap timeout`	integer (en secondes)	durée maximale d'attente d'une réponse de l'annuaire	15	Global

Tableau 8. Paramètres relatifs à LDAP

Exemple 14.

```
[Global]
    security = user
    encrypt passwords = yes
    passdb backend = ldapsam:''ldap://ldap1/ ldap://ldap2/''
    ldap_ssl = start_tls
    ldap admin dn = cn=smbadmin,ou=people,dc=example,dc=com
    ldap suffix = dc=example,dc=com
    ldap user suffix = ou=people
    ldap group suffix = ou=group
    ldap machine suffix = ou=people # on ne sépare pas les machines des utilisateurs
ici
    ldap idmap suffix = ou=idmap
```

Le mot de passe du DN de l'annuaire doit être conservé en clair dans `secrets.tdb` :

Exemple 15.

```
root# smbpasswd -W
Setting stored password for ‘‘cn=smbadmin,ou=people,dc=example,dc=com’’ in secrets.tdb
...
```

4.6. Mappage d'utilisateurs

Paramètre	Valeur	Description	Défaut	Portée
`username map`	string	chemin absolu du fichier contenant les équivalences	,,,,	Global
`username map script`	string	chemin absolu du script ou de l'outil qui accepte le nom d'utilisateur en paramètre et retourne le nom mappé	,,,,	Global

Tableau 9. Mappage d'utilisateurs

Le fichier, souvent nommé `smbusers`, a comme format : `map_to_Unix_name = ''map_from''` (les guillemets sont nécessaires en présence d'une espace dans le login.

Exemple 16.

```
[global]
    username map = /etc/samba/smbusers
    ....
```

4.7. Utilitaires de gestion des utilisateurs : `smbpasswd` et `pdbedit`

Ces outils fonctionnent de la même façon quel que soit le backend utilisé pour stocker les comptes et mots de passe. Il n'est, par exemple, pas nécessaire de remplir l'annuaire à la main (Samba doit donc être démarré lorsqu'on les utilise).

`smbpasswd` peut fonctionner selon deux modes :

- utilisé par l'utilisateur `root`, il permet de modifier les comptes des utilisateurs sur le serveur ;

  `smbpasswd [options] username`

- utilisé par un utilisateur, il permet de modifier le mot de passe crypté à distance.

  `smbpasswd [options]`

utilisateur `root`.

-a username. ajoute le compte *username* s'il existe déjà un compte Unix correspondant. Si *username* existe déjà, seul le mot de passe est modifié.

-d username. invalide *username*. Le compte existe toujours mais l'utilisateur ne peut plus s'authentifier.

-e username. autorise ou refuse l'authentification à *username*. Cette option annulé `-d username`.

-m. indique que le compte est un compte machine (déprécié).

-n. positionne le mot de passe de l'utilisateur à `null`. Pour qu'il puisse s'authentifier, il faut que la directive `null passwords = yes` apparaisse dans la section `[global]` de `smb.conf`.

-R. permet d'effectuer une résolution de nom différente de celle choisie dans `smb.conf`. Les paramètres sont identiques.

-W. enregistre le mot de passe du `ldap admin dn` de l'annuaire.

-w. identique à `-W` si ce n'est que le mot de passe n'apparaît pas sur la ligne de commande.

-x username. détruit le compte (login, mot de passe, informations, ...) *username*.

tout utilisateur.

-c filename. indique un fichier de configuration autre que smb.conf.

-D debug_level. niveau de debug.

-r NETBIOS_name. indique sur quelle machine (généralement le PDC) le compte doit-être modifié.

-s. le mot de passe n'est pas demandé, mais attendu comme paramètre. Utile dans les scripts.

```
root# (echo ‘‘cat’’; echo’’cat’’) | smbpasswd -s -a smitty
```

crée le compte *smitty* avec le mot de passe *cat* répété deux fois pour répondre aux deux questions posées par smbpasswd (valeur puis confirmation).

-U username. change le mot de passe de *username* sur une machine distante. Ce paramètre permet au compte *username* d'être différent sur les machines locales et distantes. Nécessite donc le paramètre `-r NETBIOS_name`.

`pdbedit` possède une syntaxe plus complexe que celle de `smbpasswd`. Il fournit néanmoins plus de fonctionnalité. En particulier il permet :

- de configurer les propriétés des comptes telles que la durée maximale d'existence d'un mot de passe, le nombre de mots de passe faux tolérés avant de bloquer le compte, ...
- de configurer les attributs de l'utilisateur comme les scripts de login, le SUD, la localisation des profils itinérants, ...
- de convertir le fichier de comptes d'un backend vers un autre :

```
root# pdbedit -ismbpasswd:/tmp/smbpasswd -etdbsam:/tmp/passdb.tdb
```

4.8. Synchronisation des mots de passe

De façon à modifier les mots de passe Unix des utilisateurs, `smbd` peut :

- communiquer avec un programme externe ;
- utiliser PAM ;
- demander à l'annuaire LDAP de faire la modification.

Paramètre	Valeur	Description	Défaut	Portée
`check password script`	string	script externe vérifiant la validité du mot de passe	,,,,	Global
`ldap password sync`	boolean	`smbd` envoye l'instruction à l'annuaire de modifier l'attribut mot de passe posix (seulement pour OpenLDAP)	no	Global
`pam password change`	boolean	`smbd` utilise PAM pour changer le mot de passe	no	Global
`passwd program`	string	programme externe servant à changer le mot de passe	,,,,	Global
`passwd chat`	string	chaîne de caractères que `smbd` utilise pour interagir avec le programme qui modifie le mot de passe	voir exemple	Global
`passwd chat debug`	boolean	verbosité dans les fichiers de log du processus de synchronisation	no	Global
`passwd chat timeout`	integer	durée maximale (en secondes) pour le processus de synchronisation	2	Global
`unix password sync`	boolean	définit si Samba doit tenter de synchroniser le mot de passe Unix	no	Global

Tableau 10. Synchronisation des mots de passe

Utilisation :

d'un programme externe.

Exemple 17.

```
[global]
    encrypt passwords = yes
    unix password sync = yes
    passwd program = /usr/bin/passwd %u
    passwd chat = *New*password* %n\n\
                  *Reenter*new*password* %n\n\
                  *Passwd*changed*
```

car l'utilisation de la commande `passwd` génère la sortie :

```
root# passwd lizard
Changing password for lizard.
New password:
Reenter New Password:
Passwd changed.
```

de PAM.

Exemple 18.

```
[global]
    encrypt passwords = yes
    unix password sync = yes
    pam password change = yes
    passwd chat = *New*password* %n\n\
```

```
*Reenter*new*password* %n\n\
*Passwd*changed*
```

4.9. Mappage de groupes

Création d'un groupe.

```
root# net groupmap add ntgroup=''System Managers'' unixgroup=sysadmin
```

Modification d'un groupe.

```
root# net groupmap modify ntgroup=''System Managers'' unixgroup=sysops
comment=''Server administrators group''
```

Destruction d'un groupe.

```
root# net groupmap delete ntgroup=''System Managers''
```

Énumération des groupes.

```
root# net groupmap list
```

Information sur un groupe.

```
root# net groupmap list verbose ntgroup=''Printers Admins''
```

4.10. La commande `net`

4.10.1. `net rpc`

Utilisateurs et groupes.

Option principale	Option secondaire	Paramètre	Description
user			énumère les comptes utilisateurs
	`add`	*username[password]*	crée un compte utilisateur (mot de passe possible)
	`delete`	*username*	supprime un compte utilisateur
	`info`	*username*	énumère les groupes auxquels appartient l'utilisateur
	`rename`	*oldname newname*	renomme un compte
group			énumère les groupes
	`list`	[global|local|builtin]	énumère les groupes spécifiques
	`add`	*name*	crée un nouveau groupe
	`delete`	*name*	supprime un groupe
	`members`	*name*	énumère les membres d'un groupe
	`addmem`	*group user*	ajoute l'utilisateur *user* au groupe *group*
	`delmem`	*group user*	supprime l'utilisateur *user* du groupe *group*

Tableau 11. net rpc – utilisateurs et groupes

On peut aussi préciser :

-U user. le nom d'utilisateur sous lequel on lance la recherche/commande ;

-S server. le nom NETBIOS du serveur cible ;

-w workgroup. le nom du groupe de travail cible ;

-I address. l'adresse IP du serveur cible.

Exemple 19.

```
net rpc user -S windc -U lizard # comptes utilisateurs sur windc

net rpc user info lizard -S windc -U lizard # groupes auxquels appartient lizard

net rpc user add jsmith -S windc -U Administrator # création du compte jsmith

net rpc user rename jsmith smitty -S windc -U Administrator # renomme le compte jsmith
smitty

net rpc password smitty LeAv3: -S windc -U Administrator # attribue le mot de passe LeAv3:
au compte smitty

net rpc group addmem ''Domain Admins'' smitty -S windc -U Administrator # ajoute smitty au
groupe spécifié

net rpc group members ''Domain Admins'' -S windc -U Administrator # énumère les membres du
groupe spécifié
```

Partages.

Paramètre	Options	Description
None		énumère les partages sur le serveur
add	*sharename=path*	crée un nouveau partage sur le serveur à partir du chemin spécifié
allowusers	*sharename*	liste des SID autorisés à explorer le partage
delete	*sharename*	supprime le partage sur le serveur
migrate	*<all/files/security/shares>[share]*	migre les paramétrages du partage du serveur distant au serveur local

Tableau 12. net rpc share

Exemple 20.

```
net rpc share -S windc -U Administrator # liste les partages du serveur windc

net rpc share add ''UserHome=C:\\users'' -S windc -U Administrator # crée le partage
UserHome
```

Services.

Paramètre	Options	Description
list		énumère les services installés sur le serveur
pause	*servicename*	met le service en pause (pas supporté par tous les services)
start	*servicename*	démarre le service
status	*servicename*	indique l'état du service
stop	*servicename*	stoppe le service
resume	*servicename*	redémarre le service

Tableau 13. net rpc service

Exemple 21.

```
net rpc service list -S windc -U Administrator # liste les services sur windc

net rpc service status w32time -S windc -U Administrator # état du service w32time

net rpc service stop w32time -S windc -U Administrator # stoppe le service w32time

net rpc service start w32time -S windc -U Administrator # démarre le service w32time

net rpc shutdown -r -t 120 \
    -C ‘‘Maintenance redémarrage nécessaire. Déconnectez-vous !’’ \
    -S dorn -U Administrator       # reboot dans 120 s
```

4.10.2. `net ads`

4.11. Attribution de droits spécifiques

Paramètre	Valeur	Description	Défaut	Portée
`enable privileges`	boolean	autorise ou pas l'octroie de privilèges aux utilisateurs	no	Global

Tableau 14. Attribution de droits spécifiques

Privilège	Description
`SeAddUsersPrivilege`	peut ajouter, modifier et détruire des utilisateurs. Peut aussi modifier l'appartenance à un groupe
`SeBackupPrivilege`	pas utilisé pour l'instant
`SeDiskOperatorPrivilege`	peut créer, modifier ou détruire des fichiers dans un partage. Peut aussi modifier les ACL
`SePrintOperatorPrivilege`	peut ajouter, modifier ou retirer des imprimantes
`SeMachineAccountPrivilege`	peut ajouter ou retirer une machine du domaine
`SeRemoteShutdownPrivilege`	peut éteindre ou redémarrer un serveur Samba
`SeRestorePrivilege`	peut rendre un utilisateur lambda propriétaire d'un fichier ou d'un dossier
`SeTakeOwnershipPrivilege`	peut devenir le propriétaire d'un fichier ou d'un dossier

Tableau 15. Droits spécifiques

Exemple 22.

```
net rpc rights list -S localhost -U Administrator -W AD # privilèges définis sur la machine

net rpc rights grant 'RAIN\lizard' SeDiskOperatorPrivilege \
        -S localhost -U root -W RAIN

net rpc rights list accounts -S localhost -U% # énumère tous les comptes contenus dans la
base de donnée                                                    maintenue par Samba et
les droits associés
```

4.12. Autorisations sur les partages

Paramètre	Valeur	Description	Défaut	Portée
`admin users`	*user/group list*	liste d'utilisateurs ou de groupes à qui l'on attribue tous les droits sur le partage	,,,,	Share
`invalid users`	*user/group list*	liste d'utilisateurs ou de groupes à qui l'on refuse l'accès au partage	,,,,	Share
`max connections`	Integer	nombre maximal de connexions simultanées au partage (0 signifie que l'accès n'est pas restreint)	0	Share
`read list`	*user/group list*	liste des utilisateurs ou groupes qui n'ont qu'un accès en lecture dans le partage	,,,,	Share
`valid users`	*user/group list*	liste des utilisateurs ou groupes qui ont accès au partage	,,,,	Share
`write list`	*user/group list*	liste des utilisateurs ou groupes qui ont un accès en écriture dans le partage	,,,,	Share

Tableau 16. Autorisations sur les partages

Exemple 23.

```
[document]
    path = /data/docs
    read only = no
    admin users = rose, lily, +staff
```

Remarque. tout fichier ou dossier créé dans le partage sera la propriété de root et pas de l'utilisateur de `admin users`

```
[administration]
    path = /data/administration
    read only = yes
    write list = +pcadmins
```

toute personne n'appartenant pas au groupe `pcadmins` n'a qu'un accès en lecture au partage.

```
[administration]
    path = /data/administration
    read only = no
    read list = +guest
```

les utilisateurs du groupe `guest` n'ont pas le droit de modifier le partage.

5. Options avancées

5.1. Noms des fichiers/dossiers

Sous Windows, le système de fichier *préserve* et est *insensible* à la casse. Sous Unix, ils la *préservent* et y sont *sensibles*.

Paramètre	Valeur	Description	Défaut	Portée
`max stat cache size`	integer	limite la quantité max (en ko) de mémoire allouée au «stat cache» de chaque démon smbd	0	Global
`stat cache`	boolean	si oui, Samba conserve en cache les noms des fichiers déjà recherchés avec différentes casses	yes	Global
`case sensitive`	boolean	Samba doit-il considérer que le client envoie le nom du fichier avec la bonne casse ?	no	Share
`default case`	upper or lower	quelle casse utiliser si le paramètre précédent est positionén à «yes»	lower	Share
`preserve case`	boolean	Samba doit-il écrire les noms de fichiers longs tels que les ont écrit les utilisateurs (voir `case sensitive`) ?	yes	Share
`short preserve case`	boolean	Samba doit-il conserver le format original 8.3 des noms courts ?	yes	Share

Tableau 17. Noms de Fichiers/dossiers

Exemple 24.

1. Utilisateur enregiste Foo.txt ;
2. Utilisateur recherche foo.txt.

Samba recherche foot.txt puis toutes les combinaisons possibles jusqu'à trouver Foo.txt. Ce nom est ensuite gardé en mémoire pour répondre plus vite lors d'une demande ultérieure.

```
[drawings]
    path = /data/drawings
    read only = no
    case sensitive = yes
    default case = lower
    preserve case = no
    short preserve case = no
```

On demande à Samba de ne plus préserver la casse et de systématiquement enregistrer les noms des fichiers en minuscule. On peut donc surement diminuer `max stat cache size` et on gagne du temps sur des serveurs très chargés.

Remarque. Les systèmes de fichiers sous Unix sont généralement lents lorsqu'il s'agit de lire des dossiers comportant un très grand nombre de petits fichiers. Dans ce cas, adopter la technique employée ci-dessus.

5.2. Liens symboliques

Paramètre	Valeur	Description	Défaut	Portée
`follow symlinks`	boolean	Samba doit-il suivre les liens symboliques ?	yes	Share
`wide links`	boolean	Samba doit-il suivre les liens symboliques pointant à l'extérieur du partage ?	yes	Share

Tableau 18. Liens symboliques

Pour des raisons de performances, laisser le premier paramètre à «yes».

5.3. Masquage de fichiers

Paramètre	Valeur	Description	Défaut	Portée
`delete veto files`	boolean	Samba peut-il effacer les fichiers exclus de la navigation lorsqu'on efface le dossier qui les contient ?	no	Share
`hide dot files`	boolean	quand activé, Samba positionne l'attribut «hidden» sur les fichiers ou les répertoires dont le nom commence par un point	yes	Share
`hide files`	filename pattern	Samba place l'attribut «hidden» sur les fichiers ou répertoires correspondants à l'expression régulière (ou les expressions régulières)	None	Share
`hide special files`	boolean	exclut de la navigation les fichiers spéciaux (socket, pipes, ...)	no	Share
`hide unreadable files`	boolean	exclut de la navigation les fichiers/dossiers que l'utilisateur n'a pas le droit de lire	no	Share
`hide unwriteable files`	boolean	exclut de la navigation les fichiers/dossiers que l'utilisateur n'a pas le droit de modifier	no	Share
`veto files`	filename pattern	Samba exclut de la navigation les fichiers ou répertoires correspondants à l'expression régulière (ou les expressions régulières)	None	Share

Tableau 19. Masquage de fichiers

Il existe une différence entre «cacher» de la navigation et «exclure» de la navigation : dans le premier cas l'accès au fichier reste possible si on connaît le chemin direct pour y parvenir, dans le second, il est impossible d'accéder au fichier.

Exemple 25.

```
[homes]
    read only = no
    hide files = /*.ini/*.log/
```

5.4. Verrous

5.5. Attributs DOS

5.6. Permissions

5.7. ACL

5.8. MS-DFS

C'est l'équivalent Windows de l'automonteur présent sous Unix. À utiliser donc pour répartir la charge de travail du serveur de fichiers.

Paramètre	Valeur	Description	Défaut	Portée
`host msdfs`	boolean	si activé permet à Samba de supporter MS-DFS	no	Global
`msdfs root`	boolean	si activé, Samba informe les clients que le partage est la racine MS-DFS	no	Share

Tableau 20. MS-DFS

Exemple 26.

```
[global]
    hosts msdfs = yes
[common]
    path = /data/dfs
    read only = yes
    msdfs root = yes
```

Les références vers les partages situés sur les autres serveurs de fichiers sont enregistrées sous forme de liens symboliques de la forme : `msdfs:server\share`.

```
ln -s 'msdfs:sleet\staff' staff
```

Le partage est en lecture seule puisqu'on considère qu'il ne contient que des liens symboliques (ce n'est donc pas obligatoire).

Remarque.

msdfs proxy définit un partage qui fait simplement référence à un autre partage. Par exemple si on a bougé le contenu de `\\RAIN\templates` vers `\\SNOW\`templates mais que certaines machines clientes persistent à interroger `\\RAIN`, on peut utiliser :

Exemple 27.

```
[global]
    netbios name = RAIN
[templates]
    msdfs proxy = \\snow\templates
```

5.9. VFS

5.10. Scripts

6. Résolution de noms et exploration du réseau

6.1. Résolution de noms

6.1.1. Systèmes d'exploitation windows modernes

Différentes méthodes utilisées par les systèmes d'exploitation windows modernes :

- recherche du nom dans le cache des noms récemment résolus ;

- interrogation d'un serveur DNS ;
- utilisation d'un fichier hosts ;
- interrogation d'un serveur WINS ;
- utilisation d'un fichier LMHOSTS ;
- envoi d'une demande sur l'adresse de broadcast.

6.1.2. Interaction entre un client WINS et un serveur WINS

Lorsque le client rejoint le réseau, il enregistre son nom NETBIOS auprès du serveur WINS, qui stocke l'association nom NETBIOS/adresse IP dans sa base de données (`wins.dat`). Cette entrée est notée «active».

Le client est censé, périodiquement, recontacter le serveur pour l'informer qu'il utilise toujours le nom. Cette période est appelée time to live (TTL). Lorsqu'il quitte le réseau, le client doit informer le serveur que le nom est à nouveau disponible. Dans le cas contraire, le serveur attend la fin du bail.

La base `wins.dat`, gérée par le démon `nmbd` n'est donc qu'une photo de l'état du réseau à une certaine date, elle ne traduit pas forcément fidélement la réalité à une date ultérieure (machine non correctement arrêtée, ...).

Remarque. Samba est incapable de répliquer sa base WINS vers un autre serveur.

Paramètre	Valeur	Description	Défaut	Portée
`wins support`	boolean	détermine si `nmbd` agit fait office de serveur WINS	no	Global
`wins server`	string (IP adress ou DNS name)	indique à Samba le ou les serveurs WINS à utiliser	None	Global
`wins proxy`	boolean	indique à Samba d'agir comme un proxy à un serveur WINS situé sur un autre sous-réseau	no	Global
`wins hook`	string	commande externe à exécuter lorsque wins.dat est modifiée	None	Global
`dns proxy`	boolean	permet à nmbd d'interroger un serveur DNS si le nom à résoudre ne se trouve pas dans wins.dat	yes	Global
`name resolve order`	string	dans quel ordre smbd effectue-t-il la résolution	lmhosts wins host bcast	Global

Tableau 21. Résolution de noms

- `wins support` et `wins server` sont exclusifs ;
- configuration serveur

Exemple 28.

```
[global]
```

```
    name resolve order = wins lmhosts hosts bcast
    wins support = yes
    dns proxy = yes # par défaut
    wins hook = /usr/local/bin/dns_update # voir examples/scripts/wins_hook
```

- configuration client

Exemple 29.

```
[global]
    name resolve order = wins lmhosts hosts bcast
    wins server = 192.168.1.2 192.168.1.3
    wins proxy = yes # pas toujours utile
```

6.2. Exploration du réseau

Paramètre	Valeur	Description	Défaut	Portée
`local master`	boolean	si activé, permet à Samba de participer à l'élection du Local Master Browser	yes	Global
`preferred master`	boolean	si activé, force une réélection pour permettre à Samba de devenir le Local Master Browser	yes (si à la fois master et domain browser sont activés)	Global
`domain master`	boolean	si activé, Samba devient le Domain Master Browser (*les stations win s'attendent à ce qu'il soit alors aussi PDC s'il y en a un*)	no	Global
`os level`	numeric (0-255)	niveau pour participer à l'élection	20	Global
`remote browse sync`	string (liste d'adresses IP)	dans un réseau avec sous-réseaux géré uniquement par des serveurs Samba et sans PDC, liste des Local Master Browser pour synchroniser les listes	None	Global
`remote announce`	string (liste d'adresses IP/nom des workgroup)	sous-réseaux et workgroups auxquels il faut envoyer une demande broadcast pour synchroniser les listes dans une situation équivalente à celle directement dessus. La plupart des routeurs filtrant les broadcast !!!	None	Global

Tableau 22. Exploration

Remarque. Le dhcp doit indiquer le serveur WINS et le serveur PDC (ou DMB) au minimum, afin que les LMB contactent le DMB.

LMB.

Exemple 30.

```
[global]
    local master = yes # défaut
    preferred master = yes
    os level = 20 # défaut suffisant si pas d'autres Samba, choisir sinon un nombre >
20 et < 33 (DMB donc PDC)
```

DMB donc PDC.

Exemple 31.

```
[global]
    domain master = yes
    preferred master = yes
    local master = yes
    os level = 33
```

Le DMB est donc LMB de son sous-réseau.

Quelques règles à retenir pour améliorer l'exploration.

- Placer un serveur Windows NT ou Samba faisant office de LMB dans chaque sous-réseau du groupe de travail/domaine ;
- Utiliser un PDC faisant office de DMB ;
- Utiliser un serveur WINS.

7. CONTRÔLEUR DE DOMAINE

7.1. Configuration du PDC

1. Choisir le mode de sécurité `user` : `security = user` ;
2. Forcer l'utilisation des mots de passe cryptés : `encrypt passwords = yes` ;
3. Définir un partage `[netlogon]` ;
4. Configurer la machine comme « explorateur principal de domaine » (DMB) : `domain master = yes` ;
5. Configurer la machine comme serveur de « logon » : `domain logon = yes`

Activer le paramètre `domain master` oblige `nmbd` à s'enregistrer comme `DOMAIN<0×1b>` auprès du serveur WINS. Ce nom est utilisé par les clients Windows pour localiser le PDC qui, lui, est enregistré comme `DOMAIN<0×1c>`. C'est le rôle du paramètre `domain logon` que d'obliger `nmbd` à s'enregistrer comme tel.

Exemple 32.

```
[global]
    netbios name = STORK
```

```
    workgroup = ORA
    security = user
    encrypt passwords = yes

    # enable PDC functionality
    domain master = yes
    domain logons = yes

    # local master browser
    os level = 33
    preferred master = yes
    local master = yes

[netlogon]
    comment = Net Logon service
    path = /data/netlogon
    read only = yes
    write list = +ntadmin
```

Exploration du réseau.

```
nmblookup 'COROT#1b' 'COROT#1c'
```

Il reste à :

1. Créer un groupe « Administrateurs de domaine » : `Domain Admins` ;
2. Associer des utilisateurs à ce groupe ;
3. Implémenter l'infrastructure de gestion des comptes machines.

Domain Admins.

Ce groupe doit toujours posséder un RID de 512. Tout membre de ce groupe est automatiquement administrateur des machines du domaine.

Exemple 33.

Obtention du SID du domaine :

```
# net getlocalsid COROT
SID for domain COROT is : S-1-5-21-3489264249-1556752242-1837584028
```

Ajout du RID du groupe au SID du domaine, pour la création du SID du groupe :

```
net groupmap add sid=S-1-5-21-3489264249-1556752242-1837584028-512 \
ntgroup=''Domain Admins'' unixgroup=ntadmin
```

Gestion des privilèges.

1. Mapper un groupe Unix à un groupe Windows ;
2. Attribuer le privilège souhaité au groupe Windows (utiliser un compte du groupe `Domain Admins`, ici cindy) ;

Exemple 34.

Création d'un groupe ayant le droit d'intégrer une machine dans le domaine

```
# net groupmap add unixgroup=srvadmin ntgroup=''Server Admins''
# net rpc rights grant 'COROT\Server Admins' SeMachineAccountPrivilege \
  -S stork -U cindy
```

8. PROGRAMME SMBCLIENT

Liste des partages publiés par une machine.

```
smbclient -L WinClient -U username
smbclient -L WinClient -U username%password
smbclient -L WinClient -A /home/.../filename
```

La seconde commande est à éviter puisque le mot de passe apparaît en clair (et reste dans l'historique des commandes). Il est donc possible, comme dans la troisième commande, d'utiliser les paramètres de connexion dans un fichier au format :

```
username = <value>
password = <value>
domain = <value>
```

Découverte du contenu d'un partage.

```
smbclient //server/partage -U username
smbclient //server/partage -A /home/.../filename
```

Envoie d'un message à l'utilisateur d'une machine.

```
cat myMessage.txt | smbclient -M nomMachine
```

ici le message est contenu dans le fichier `myMessage.txt`. Les options `-U` et `-I` permettent de contrôler les parties `FROM` et `TO` du message.

Backup.

```
smbclient //myPC/myShare `` `` -N -Tx backup.tar
```

restore depuis l'archive `backup.tar` dans `myShare` sur `myPC` (aucun mot de passe sur le partage).

```
smbclient //myPC/myShare `` `` -N -TXx backup.tar users/docs
```

restore tout depuis l'archive `backup.tar` dans `myShare` sur `myPC` excepté `users/doc` (aucun mot de passe sur le partage).

```
smbclient //myPC/myShare `` `` -N -Tc backup.tar users/docs
```

crée une archive `backup.tar` de tous les fichiers dans `users/docs`.

```
smbclient //myPC/myShare `` `` -N -Tc backup.tar users\docs
```

idem mais avec un chemin de type DOS.

`smbclient //myPC/myShare `` `` -N -TcF backup.tar tarlist`

crée une archive `backup.tar` de tous les fichiers dont le nom est dans le fichier `tarlist`.

`smbclient //myPC/myShare `` `` -N -Tc backup.tar *`

crée une archive contenant tous les fichiers et répertoires du partage.

Remarque 35. l'option `-N` est pratique car elle supprime la demande de mots de passe pour les partages n'en demandant pas.

ftp. `smbclient //server/share -U username`

? [command]. informations sur la commande.

! [shell command]. lance une commande dans un shell local à la machine sur laquelle on travaille.

chown file uid gid. cette commande dépend des caractéristiques du serveur distant.

chmod file <mode in octal>.

del <mask>. détruit tous les fichiers correspondant au masque dans le partage.

dir <mask>. liste les fichiers correspondant au maque dans le partage.

get <remote file name> [local file name]. copie le fichier `remote file name` du serveur vers la machine locale.

lcd [directory name]. permet de lister ou changer de répertoire sur l'ordinateur local.

mget <mask>. copie tous les fichiers correspondant au masque depuis le serveur.

mkdir <directory name>.

mput <mask>. copie tous les fichiers correspondant au masque depuis la machine locale vers le serveur.

print <file name>. imprime le fichier de la machine locale vers un serveur d'impression.

put <local file name> [remote file name].

recurse. établi ou supprime la récursion pour les commandes `mput`, `mget`, `rm` et `rmdir`.

Exemple de sauvegarde de tout un partage :

```
smbclient //server/share -U username
> prompt
> recurse
> mget *
```

S'il existe plusieurs domaines, utiliser les options `-n netbiosname -W workgroup`.

Remarque 36. On peut changer la taille du buffer utilisé par smbclient.

```
smblcient -b buffer_size //server/share [password] [options]
```

9. MONTAGES CIFS

/etc/fstab.

```
//server/share /mnt/local_folder cifs user,noauto,credentials=/etc/.../filename,
uid=500,gid=500 0 0
```

Syntaxe de filename.

```
username = <value>
password = <value>
```

Remarque 37. forcer l'uid et le gid s'ils sont différents sur le serveur et sur la machine locale. Ceci ne fonctionne pas si le serveur supporte les «CIFS Unix extensions» (si problème utiliser `unix extensions = no`).